

Privacy Policy

How Adovasio Technology LLC collects, uses, stores, and protects information across its websites, applications, and online services.

Effective: August 10, 2026

This Policy is intentionally service-wide. It applies to Adovasio-owned or Adovasio-operated websites, domains, subdomains, mobile applications, software, APIs, and online services that link to or expressly adopt this Policy (collectively, the "Services"), including future Services. It does not automatically apply to a client-owned website or service merely because Adovasio built, hosts, or supports it.

No sale of personal data Adovasio does not sell personal data. Adovasio does not currently use third-party advertising networks on its websites.	Accounts and storage Account data is generally retained while an account is active. After account deletion, active-service account data is generally scheduled for deletion within 30 days, subject to legal, security, and backup exceptions.
Payments Payment providers such as Stripe, PayPal, Venmo, Apple, or other processors may collect payment credentials directly. Adovasio generally receives transaction and limited payment metadata rather than full card credentials.	Privacy requests Requests for access, correction, portability, or deletion may be sent to privacy@adovasio.com.

Important service-specific notices

Not every data category or feature described below applies to every Adovasio Service. A Service may present an additional, more specific privacy notice when its functionality requires one. If a service-specific notice conflicts with this Policy for that Service, the more specific notice controls for that processing.

1. Who We Are and Scope

Adovasio Technology LLC ("Adovasio," "we," "us," or "our") operates technology services for individuals and businesses. This Privacy Policy explains our practices when Adovasio acts as the operator or controller of a Service.

This Policy also covers information processed through an Adovasio account or single sign-on system, including sso.adovasio.com, when that information is used to provide access to Adovasio Services.

A third-party or client-owned website, app, or system may have its own privacy policy even if Adovasio provides hosting, development, IT support, or infrastructure for that party. In those situations, the client or other third party may be the controller of the information and its privacy notice should be reviewed separately.

2. Information We Collect

Account and identity information

When you create or use an account, we may collect information such as your name, email address, telephone number, username, account identifiers, authentication status, security settings, and authentication credentials. Passwords and similar credentials are handled as security-sensitive authentication data and are not intended to be stored or displayed in readable plaintext.

Payment and transaction information

If you purchase an Adovasio product or service, payment information may be collected by a payment provider such as Stripe, PayPal, Venmo, Apple, or another provider presented at checkout. Depending on the payment method, the provider may collect card numbers, bank or wallet information, billing details, and fraud-prevention information directly. Adovasio generally receives information such as the payer name, contact information, transaction identifier, amount, payment status, payment method type, and limited payment details (for example, card brand and last four digits) rather than a complete card number or security code.

Files, photos, prompts, messages, and other content

Many Services allow you to upload, store, convert, analyze, transmit, or generate content. This may include documents, images, photographs, videos, files, text, prompts, messages, AI conversations, metadata, generated outputs, and other information you choose to provide. The content processed depends on the Service you use.

Device, network, and technical information

We may automatically receive technical data such as public IP address, browser and device type, operating system, app version, requested URL, referring page, timestamps, session identifiers, error logs, security events, network metadata, and similar diagnostic information. This information may be generated by web servers, firewalls, web application firewalls, content delivery networks, authentication systems, and other infrastructure used to operate and protect the Services.

Communications and support information

If you contact Adovasio, request support, submit an inquiry, or otherwise communicate with us, we may retain the content of the communication and related contact information as reasonably necessary to respond, provide support, document the interaction, and protect our legal and security interests.

Mobile app data and permissions

An Adovasio mobile application may collect or access device information or content only as needed for its features and subject to the permissions you grant through the device or operating system. Depending on the app, this could include photos, camera access, files, notifications, device identifiers, diagnostics, or other app-specific data. The applicable app interface and app-store privacy disclosures provide additional detail for that app.

3. How We Collect Information

- Directly from you, including when you create an account, upload content, use a tool, make a purchase, or contact us.
- Automatically from your browser, device, app, or network connection when you access or use a Service.
- From payment processors, app stores, authentication providers, or other service providers when necessary to complete a transaction or provide the Service.
- From a business customer, organization administrator, or other authorized party that creates or manages an account for you.

4. How We Use Information

We use personal information for purposes that include:

- Providing, operating, maintaining, and improving the Services and their requested functionality.
- Creating, authenticating, securing, administering, and supporting user accounts.
- Processing purchases, subscriptions, invoices, refunds, and other transactions.
- Processing uploaded files or content, delivering generated output, synchronizing data, or storing content when the Service is designed to provide storage.

- Sending service-related communications such as sign-in codes, two-factor authentication messages, password resets, security alerts, receipts, service notices, and support responses.
- Detecting, investigating, and preventing fraud, abuse, malware, unauthorized access, attacks, and other security threats.
- Diagnosing errors, maintaining reliability, measuring service performance, and planning capacity.
- Complying with law, enforcing agreements, resolving disputes, and protecting Adovasio, our users, and others.
- Performing other purposes that we disclose at the time information is collected or for which you provide valid consent.

Adovasio does not currently use personal information for solely automated decisions that produce legal or similarly significant effects on individuals. If that changes for a Service, we will provide any notice and choices required by applicable law.

5. AI and Automated Features

Some Services may include artificial intelligence, machine learning, automated analysis, or similar features. Information you submit to such a feature - including prompts, files, messages, or other content - may be processed by the software, model, infrastructure, or service provider needed to generate the requested response or result.

AI features may produce inaccurate, incomplete, or unexpected output. This Privacy Policy describes data handling; separate Terms of Use govern reliance on output and other conditions of use. Where an app or Service sends personal data to a third-party AI provider, Adovasio will provide additional disclosure when required by applicable law or platform rules.

6. Cookies, Cloudflare, and Similar Technologies

Adovasio Services may use cookies, local storage, session identifiers, and similar technologies that are necessary for authentication, security, preferences, fraud prevention, and core functionality. Security or content-delivery providers may also process technical information or set security-related cookies when their services are enabled.

Adovasio uses Cloudflare on some Services for functions such as content delivery, network performance, traffic management, and security. Cloudflare may process IP addresses, request metadata, security signals, and similar technical information in connection with those functions.

As of the effective date of this Policy, Adovasio does not use Google Analytics on its websites and does not use third-party advertising networks on its websites. If those practices materially change, this Policy will be updated as appropriate.

7. Advertising and Tracking

Adovasio does not sell personal data. Adovasio does not currently use website visitor data for third-party targeted advertising.

Some current or future Adovasio mobile applications may display advertising. If an app uses a third-party advertising provider, tracking technology, or advertising identifier, the app will provide the disclosures, controls, and platform permission prompts required for that implementation. Adovasio will not knowingly sell a minor's personal data or use a known minor's personal data for targeted advertising where prohibited by law.

Where applicable law provides a right to opt out of sale, targeted advertising, or certain profiling, you may exercise that right through the method presented in the applicable Service or by contacting privacy@adovasio.com. Where legally required, Adovasio will also honor qualifying universal opt-out preference signals for applicable processing.

8. How We Share Information

We may disclose personal information to the following categories of recipients when reasonably necessary for the purposes described in this Policy:

- **Infrastructure, hosting, and security providers.** Providers that help deliver, secure, monitor, or operate the Services, including content-delivery, network, cloud, hosting, email-delivery, authentication, monitoring, and security services. Cloudflare is one example used by some Adovasio Services.
- **Payment and commerce providers.** Providers such as Stripe, PayPal, Venmo, Apple, and other payment or app-distribution providers involved in a transaction.
- **Service-specific technology providers.** A Service may rely on third-party software, APIs, communications providers, or other vendors to perform requested functionality. When material, those relationships may be described in the Service itself or an additional notice.
- **Professional advisers and legal authorities.** Lawyers, accountants, insurers, auditors, regulators, law enforcement, courts, or other persons when reasonably necessary to obtain advice, protect rights, respond to lawful process, or comply with law.
- **Business transactions.** A buyer, successor, financing source, or adviser in connection with an actual or proposed merger, acquisition, financing, reorganization, asset sale, or similar transaction, subject to appropriate safeguards where required.

We may also disclose information at your direction or with your consent. We do not disclose personal information to third parties simply for them to sell it as their own product.

9. File and Content Retention

Persistent-storage Services

For Services designed for ongoing storage - for example, an account-based photo or file storage service - user content is generally retained while the account remains active. If the account is deleted, associated active-service content is generally scheduled for deletion within 30 days, subject to the exceptions below.

Temporary-processing Services

For Services designed primarily to convert, transform, analyze, or otherwise process a file temporarily, working copies may be retained only as long as reasonably necessary to complete processing, deliver the result, maintain short-lived caches, prevent abuse, troubleshoot failures, or satisfy other operational needs. The exact interval can vary by Service and implementation. A service-specific retention notice, if presented, controls over this general description.

Logs, backups, and legal records

Security logs, transaction records, accounting records, abuse-prevention records, and limited backup copies may be retained longer than active account data when reasonably necessary for security, fraud prevention, disaster recovery, tax or accounting requirements, legal obligations, dispute resolution, or enforcement. Backup data may persist until the applicable backup is rotated or expires and is not ordinarily restored except for continuity or disaster recovery purposes.

10. Data Retention Generally

Unless a Service states a different period, we retain personal information only for as long as reasonably necessary for the purpose for which it was collected, while an account is active, and for legitimate security, legal, accounting, or operational needs afterward.

When you request account deletion, Adovasio will close or disable the affected account and generally schedule associated active account data for deletion within 30 days. Certain information may be retained longer where required or permitted by law, including transaction, tax, fraud-prevention, security, dispute, and backup records.

11. Security

Adovasio uses administrative, technical, and organizational safeguards that are intended to protect information against unauthorized access, alteration, disclosure, or destruction. Safeguards may include encrypted network connections, access controls, authentication controls, network security systems, logging, backup procedures, and other measures appropriate to the Service and data involved.

No system, transmission method, or storage technology can be guaranteed to be completely secure. You are responsible for protecting your account credentials and for promptly notifying Adovasio if you suspect unauthorized account access.

12. Sensitive Information and User-Submitted Data

Some Adovasio Services can technically process information that may be sensitive. Unless a Service is specifically designed for that type of information, we discourage uploading Social Security numbers, full payment-card credentials, medical records, passwords, authentication secrets, private cryptographic keys, highly confidential business information, or other unusually sensitive data.

If you choose to submit sensitive information to a Service, you are responsible for ensuring that you have authority to provide it and that use of the Service is appropriate for the information. Adovasio will process user-submitted information to provide the requested functionality and for the other purposes described in this Policy, subject to applicable law. Adovasio does not sell consumer health data or use it for targeted advertising.

13. Your Privacy Choices and Requests

You may contact privacy@adovasio.com to request access to, correction of, deletion of, or a portable copy of personal information associated with you, or to exercise another privacy right provided by applicable law.

We may need to verify your identity before completing a request. We may deny or limit a request where applicable law permits or requires us to do so, such as where information must be retained for security, fraud prevention, legal obligations, or to complete a transaction you requested. If applicable law gives you a right to appeal a denial, you may appeal by replying to our decision or emailing the same address with the subject "Privacy Appeal."

A deletion request generally results in the associated account being shut down and active account data being scheduled for deletion within 30 days, subject to the retention exceptions described above.

14. Connecticut Privacy Rights

Where the Connecticut Data Privacy Act (CTDPA) applies, Connecticut consumers may have rights to confirm whether Adovasio processes their personal data, access that data, correct inaccuracies, request deletion, obtain a portable copy, and opt out of covered sale, targeted advertising, or qualifying profiling. Applicable consumers may also have rights relating to appeals and information about third-party sales. Adovasio does not sell personal data.

Connecticut law also provides additional protections for minors. Adovasio does not operate the Services as services directed to children, and we do not knowingly sell minors' personal data or knowingly use minors' personal data for targeted advertising where prohibited. Additional protections or consent requirements will be applied where required and where Adovasio knows or is required to treat a user as a minor.

15. Other U.S. State Privacy Rights

Residents of certain U.S. states may have additional rights under their state privacy laws. Depending on the law and whether it applies to Adovasio or the relevant processing, these rights may include access, correction, deletion, portability, opt-out rights, appeal rights, and rights concerning sensitive data. You may submit a request using privacy@adovasio.com.

Adovasio will not discriminate against you for exercising a privacy right protected by applicable law.

16. EEA, EU, and UK Users

Adovasio is established in the United States and does not actively market its general services outside the United States, although some Adovasio applications may be available through app stores in the European Economic Area, European Union, or United Kingdom. Where the GDPR, UK GDPR, or another applicable data-protection law applies to Adovasio's processing, Adovasio will process personal data under an available legal basis and provide the rights required by that law.

Legal bases

Depending on the processing, the legal basis may include performance of a contract or steps requested before entering a contract; legitimate interests in operating, securing, supporting, and improving the Services; compliance with legal obligations; or consent where consent is required.

Rights

Where applicable, you may have rights to access, rectify, erase, restrict, or receive a portable copy of personal data; object to certain processing; withdraw consent for processing based on consent; and lodge a complaint with your local data-protection supervisory authority. Rights are subject to the conditions and exceptions in applicable law.

International transfers

Because Adovasio is a U.S. company, information may be processed or stored in the United States. Our providers may also process information in other countries. Where legally required, applicable transfer safeguards or recognized transfer mechanisms will be used by Adovasio or the relevant provider.

17. Children and Minors

The Services are general-audience services and are not directed to children under 13. Adovasio does not knowingly collect personal information online from a child under 13 without the authorization required by law. If we learn that an under-13 user has provided personal information in circumstances requiring parental consent, we may suspend the account and delete or otherwise handle the information as required by law.

Users between 13 and the age of legal majority may use a Service only when permitted by applicable law and the applicable Terms of Use. Additional privacy restrictions may apply to known minors, including restrictions on targeted advertising, sale of personal data, profiling, direct messaging, or precise geolocation where required by law.

18. Third-Party Links and Services

The Services may link to or interoperate with third-party websites, apps, payment services, app stores, or platforms. Their privacy practices are governed by their own notices. This Policy does not control a third party's independent collection or use of information.

19. Changes to This Policy

We may update this Privacy Policy as our Services, technology, vendors, or legal obligations change. The current version will identify its effective or last-updated date. If a change materially affects how we use personal information, we will provide additional notice when required by applicable law before applying the materially different practice.

20. Contact Us

For privacy questions, requests, or concerns, contact:

Adovasio Technology LLC

privacy@adovasio.com

Privacy Policy: <https://adovasio.com/privacy>

If you are contacting us about an account, please use the email address associated with that account when possible. Do not send passwords, full payment-card numbers, private keys, or other authentication secrets by email.